General Data Protection Regulation (GDPR) Articles 33 & 34

How to expedite compliance with Rapid7 solutions

Does your organization handle the personal data of EU citizens (regardless of your geographic location)? Chances are you're already prepping for the General Data Protection Regulation (GDPR). We know GDPR compliance is no small undertaking—that's why Rapid7 has solutions and services to support you along the way. Articles 33 and 34 of the GDPR require data controllers to report personal data breaches to a supervisory authority without undue delay and, where feasible, within 72 hours of breach discovery. Additionally, data controllers must also communicate to the affected EU citizens if there is a high risk that the breach will affect their "rights and freedoms."

Solid breach responsiveness is clearly vital, but the best offense is a good defense. Ideally organizations would prefer for these processes to not be invoked in the first place. And, to state the obvious, breaches don't start and end at notification; you need to have the right people, processes, and technology to be able to detect, investigate, and respond.

Our experts have stellar backgrounds in incident response, averaging over ten years of experience, as well as unparalleled understandings of the attacker mindset. This wealth of knowledge doesn't just manifest via our services offerings—our technologies are built on this expertise.

OUR SOLUTIONS

InsightIDR: The SIEM You Always Wanted

InsightIDR, our User Behavior Analytics (UBA)-powered SIEM solution, was crafted based on our team's incident response experience. InsightIDR enables you to detect attackers earlier in the attack chain using advanced user behavior analytics, endpoint detection and response, and deception technologies. Investigations are a breeze with visual search and meaningful context. The last thing we want is hundreds of noisy, meaningless alerts every day, so we've saved you from them as well. Unlike traditional SIEM projects, our customers are up and running in a few hours—not months or years.

Don't take our word for it: See the difference for yourself with a free 30 day trial of InsightIDR, which includes a step-by-step walkthrough (and no need to wade through endless pages of documentation).

Incident Response Services

Just getting started with your incident response program, or looking to improve what you have in place today? We can provide valuable insight regardless of where you are in the process. Rapid7's Incident Response Program Development services are flexible to your individual needs and challenges. We also have a multitude of Incident Response services that include tabletop exercises, compromise assessments, and blocks of incident response retainer hours. Our experts can be counted on when you need them most—even in the face of the worst.

Rapid7 IR Retainer SLA response times include:

- 1 hour to speak with the incident response manager and begin gathering information
- 24 hours for the incident response team to assemble and begin remote investigation
- 48 hours to respond on-site after a request for on-site support (North America)

Managed Detection and Response

Don't have the time or resources to hunt for threats and attackers? We've got you covered. Whether it's day or night, weekday or weekend, our Managed Detection and Response service monitors your environment for malicious behaviors that—left undetected—could lead to a disastrous data breach. Should an incident be detected, our skilled team will automatically pivot from detection to response and work with you hand-in-hand to contain and remediate the threat.

GDPR mandates that if a data breach involving personal data has been discovered, an organization has 72 hours to gather all related information and report data breaches to the relevant regulator. Unlike traditional MSSP services, if any anomalous behavior is found in your environment, our team will both notify you and further investigate—that includes analysis of raw logs, forensic endpoint artifacts, and what we're seeing across customers and our research.

Article 33 also specifies the type of information the breach notification must include, which ranges from the nature of the incident to likely consequences and proposed remediation. As part of our investigative process, you'll receive a Findings Report, containing written analysis, criticality, raw details, as well as remediation and mitigation recommendations. MDR includes full access to InsightIDR—your team can create compliance dashboards, search and visualize logs, and view user behavior across your network.

Rapid7 MDR SLA response times include:

- 1 hour to receive, validate, and alert on critical investigative leads generated
- 1 hour to begin an incident escalation after receiving customer approval

YOUR GDPR JOURNEY DOESN'T END HERE...

Gain confidence that your team is prepared for GDPR compliance; have our experts perform a GDPR Readiness Assessment.

Need help with other facets of GDPR compliance?
Check out our GDPR Compliance Toolkit.

About Rapid7

With Rapid7, technology and security professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. To learn more about Rapid7, visit www.rapid7.com.

ENLIST OUR EXPERT TEAM (OR JUST LEARN MORE)

North America: +866.7.RAPID7 | sales@rapid7.com
EMEA: +44.118.207.9300 | emeasales@rapid7.com
APAC: +65.3159.0080 | apacsales@rapid7.com

Learn More: www.rapid7.com/gdpr